ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

2004.6, BUILDING SECURITY AND ELECTRONIC ACCESS

EFFECTIVE:	1/28/2018
RESCINDS:	2004.5
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	SUPPORT SERVICES MANAGER
ACCREDITATION CHAPTERS:	NONE
CHIEF OF POLICE:	ORLANDO ROLÓN

CONTENTS:

POLICY:

It is the policy of the Orlando Police Department that unauthorized persons are prevented from entry to non-public areas within Orlando Police Headquarters (OPH). This directive establishes a secure work environment for all Orlando Police Headquarters employees, allowing the Agency to monitor the safe and efficient flow of citizens conducting business within OPH and all community police offices.

PROCEDURES:

1. GENERAL SECURITY

All electronically-secured doors must be opened with an issued access control card. To move throughout the building and community police offices, plainclothes employees shall display their access card with attached picture identification on the outermost piece of clothing. Uniformed employees shall carry and use their access card to move throughout the building and community police offices. Employees shall ensure that unauthorized persons do not follow any employee through a secured door. All employees remain responsible for the security of their assigned work areas and for locking doors to those areas as may be necessary. When an employee has a name change, the ID unit must be notified within seven calendar days; a new access card must be issued.

1.1 CRIMINAL INVESTIGATIONS DIVISION

Due to confidential material and accreditation standards, detectives assigned to CID shall not allow any victim, suspect, or witness to be in any work area, including the assigned detective's desk. All business that needs to be conducted involving any suspects, witnesses, or victims shall be conducted in an interview room.

1.2 VENDORS

Any repeat vendors who have access into any police building will have, at minimum, a background check performed on them before they are able to move freely in the building. If a background check has not been completed prior to their arrival, they must be logged in and escorted. The Support Services Manager, or his/her designee, will ensure that all background checks have been completed on all vendors. If a new vendor is added to the vendor list, the Support Services Manager must be notified within 24 hours via email. If a vendor has any convictions, as stated but not limited to City Policy 808.31 Section D "Isolated Positions/Shifts," that vendor will not be allowed in any OPD building. All repeat vendors will have a picture access card that will be assigned to them. Before being allowed to obtain their assigned access card, all vendors must sign in at the Quartermaster window and must show a photo identification,

which shall be logged. All Quartermaster personnel who work the supply window will fill out the appropriate vendor log (Attachment A) and file it in the Quartermaster Unit. In addition, Quartermaster Unit personnel shall immediately inform the ID Unit if a vendor fails to return an access card when leaving the building for the day. No vendor is allowed to use another company representative's access card. The vendor sheet will be checked for any changes with the property supervisor on a monthly basis.

1.3 MODIFICATIONS

Modifications, upgrades, or additions to building security, which includes any community polices offices, must be coordinated with the Support Services Manager; this includes electronic access card readers and vehicle gates. Video surveillance additions and/or modifications shall be coordinated through the Criminal Investigations Division's Technology and Forensics Unit.

2. SECURED ACCESS

2.1 OPH PUBLIC ENTRANCE

OPH public areas shall be monitored via the OCULARIS Surveillance System. All video surveillance are recorded and filed for up to thirty days of an incident. Any internal requests for recorded video surveillance shall be submitted, via email, to CID's Technology and Forensics Unit Supervisor. Public areas will be open from 0800hrs to 1700hrs Monday thru Friday. OPH lobby doors are on an automated open and closed schedule that is preset during business hours

2.2 ELEVATOR SECURITY DOORS

The Lobby elevator will be access controlled to prevent visitors from entering restricted areas. All visitors shall be escorted by a representative from the appropriate unit before being allowed access into the lobby elevator. This includes any officer or agent from another law enforcement agency (e.g., OCSO, FBI, etc.).

2.3 QUARTERMASTER UNIT

Quartermaster personnel will maintain a list of specific vendors authorized to receive an access card. Upon issuing a vendor's badge, proper identification must be shown and documented in the vendor log (Attachment A). Quartermaster Unit personnel will not escort visitors; a representative from the appropriate unit shall be responsible for escorting visitors.

2.4 ALL OTHER INTERIOR DOORS

Access doors to all floors within OPH and all other OPD buildings will remain locked and secured at all times. Certain doors inside OPH and other OPD buildings are equipped with electronic access (e.g., Information Desk, SED).

3. VISITORS

Information Desk Personnel will record visitor's badges on the OPD Daily Temporary Visitor Pass Log (see attachment B) and will issue the appropriate badge to visitors that have received OPD authorization. Prior to issuing a visitor's badge, proper identification must be shown and documented in the log.

Visiting plainclothes law enforcement officers on official (non-training) business will wear their own departmental identification card or badge on their outermost piece of clothing unless in an undercover status (e.g., MBI, DEA, ICE, etc.). Any person coordinating the use of any classroom or other area inside Orlando Police Headquarters for a large group (e.g., CPA, press conference, tour group, LEBA Bike School) will be responsible for ensuring that all non-OPD persons are signed in. The Community Relations supervisor will be responsible for ensuring that all non-OPD persons are signed in at the awards ceremony. Any person inside OPH who is not an OPD employee shall be escorted and will wear a visitor's badge or their City of Orlando identification. The Information Desk personnel shall not escort visitors; a

representative from the appropriate unit shall be responsible for escorting visitors. Employees shall question any visitor not displaying identification and ensure that they are signed in at the appropriate location.

It is the responsibility of the division commanders at each community police office to maintain the visitor's log for that office.

4. ACCESS CONTROL CARDS AND IDENTIFICATION CARDS

4.1 ISSUANCE OF CARDS

The ID Unit will issue and log all access control cards through a computer database system located within the ID Unit. The Records Unit supervisor/designee shall ensure that photographs are saved and maintained. All sworn and civilian police employees, and those non-OPD employees designated by the Chief of Police, will be issued an access control card (i.e., volunteers, repeat vendors). OPD Employees **non-medically** separating with less than 20 years of service are not entitled to a "retired" identification card. To ensure building security and integrity, all personnel will be allowed only one active access card at a time; multiple cards will NOT be issued. Newly-hired personnel will be issued the access rights corresponding to the security group assigned to their position. If additional access rights are needed, it will be the responsibility of the hiring authority to notify, via email, the Support Services Manager and/or the Records Unit supervisor/designee. The email shall include the employee's name, identification number, and access control area requested. In addition, it will be the responsibility of the hiring authority to notify, via email, the Support Services Manager and/or the Records Unit supervisor/designee, when access is to be deactivated. When a new employee identification card is issued to an individual, a photo of the individual, along with the appropriate data attached, will be forwarded to the Internal Affairs Unit.

4.2 TRANSFERS/ACCESS CHANGES

All employees seeking an access change must submit a request via their chain of command to the division commander who controls the area to which access has been requested. Division Commanders shall forward the appropriate email to the Support Services Manager and/or the Records Unit supervisor/designee to change any level of employee or non-employee access. The email shall include the employee's name, identification number, and access control area change.

4.3.1 TEMPORARY ACCESS CARD

Should an employee lose or damage their access card or should the access card no longer work during non-business hours, the employee will need to obtain a temporary access card from the Quartermaster Unit. Specific temporary access cards will be issued by the Quartermaster Unit depending on your job description. On the following business day, that employee should contact the ID Unit to resolve his or her issue. The employee is responsible for signing his or her temporary access card back into the Quartermaster Unit after he or she receives a new card. If the card is not returned within five calendar days, the Support Services Manager will be notified in writing by the Quartermaster Unit with the employee's name, employee number, and the temporary access card number issued. A copy of this memo will be forwarded to the employee's supervisor.

4.3.2 DAMAGE REPLACEMENT

Replacement of a damaged card, or one that no longer operates, shall be completed by presenting the damaged card to the ID Unit. Employees are responsible for paying a nonrefundable $10 fee for a replacement card if the employee caused the damage. Replacement of a damaged "retired" identification card will require an employee verification check through a computer database system and current State Identification. A retired member not found in a computer database will be directed to the Support Services Manager or his/her designee.

4.3.3 LOST OR STOLEN CARDS

Any time an access card is lost or stolen, the Support Services Manager and/or the Records Unit supervisor/designee, must be notified immediately via email. The Support Services Manager and/or the Records Unit supervisor/designee, will run a report to make sure unauthorized access has not been gained into any buildings. The card will be immediately deactivated to ensure security integrity. There will be a nonrefundable $10 charge for cards not lost in the line of duty. This shall be paid directly to the ID Unit. No INOI shall be generated for the loss of an access control card. If the access card was lost in the line of duty, the employee shall complete a Risk Management form and incident report as well as writing an email to the Support Services Manager by the end of the tour of duty. The employee should then take the completed Risk Management form and incident report to the ID Unit for a replacement. The employee will not be assessed a fee. If the employee finds their lost access card, it shall be returned immediately to the ID Unit.

4.4 ACCESS CARD OPERATION

The access control cards will allow employees to hold the card within a 4-6 inch distance from the card reader to activate the unlocking mechanism. Once the card has been "read," the employee's information will be maintained in a database, to include which door was activated and the date/time of entry. All employees are responsible for the activity and security of their cards, and for this reason, there shall be no "loaning out" of an access card. If a card reader does not work, the Support Services Manager shall be contacted immediately via telephone or email.

4.5 RETIREE ACCESS CARD

With the Chief of Police's approval, retirees will have access to the following: the Woods Avenue and Anderson Street OPH gates, the doors leading to the break room, front lobby and Fitness Center. Retiree access will be from 0800 hours to 2000 hours, seven days a week. The Chief of Police may grant additional access. OPD Employees **non-medically** separating with less than 20 years of service are not entitled to a "retired" identification card. If a retiree's access card is lost or stolen, the retiree is responsible for notifying the ID Unit immediately.

4.6 TEMPORARY INTERNAL AFFAIRS (IA) ACCESS CARDS

No person will be allowed to check out any temporary access card from the Quartermaster Unit if relieved from duty. Internal Affairs will issue a temporary access card with restricted access to involved employees.

5. VIDEO SURVEILLANCE

These cameras will be monitored at the appropriate locations. These cameras are to provide additional security and protection for employees at OPD. If the security cameras or recorder malfunction, it shall be brought to the immediate attention of a supervisor who will then contact the Criminal Investigations Division's Technology and Forensics Unit. Employees of the Department will not alter, remove, install, or deactivate any current or proposed Department security camera without prior approval, in writing, from the Criminal Investigations Division's Technology and Forensics Unit.

6. SECURITY GROUPS

Every employee will be assigned to a security group as designated by the Support Services Manager and approved by the Building Operations Committee. Employees will have a security clearance level depending on their current work assignment. The Support Services Manager will maintain a current list of the building security levels and access. The security groups are as follows:

1. OPD COMPUTER OPERATIONS – This group shall include all Computer Operations personnel from the Help Desk at City Hall as designated by the Computer Operations Manager.

2. OPD COP – This group shall include all active Citizen Observer Program (COP) members.

3. OPD CPAA – This group shall include all active Citizen Police Academy Alumni (CPAA) members. "Active" shall be defined in the CPAA by-laws.

5. OPD CRIMELINE – This group shall include all active civilian Crimeline employees including any TDY position from other agencies.

6. OPD CSO – This group shall include all Community Service Officers (CSO).

7. OPD CSI – This group shall include all Crime Scene Investigators (CSI)

8. OPD SED GATES – This group shall include all sworn personnel, CSOs, CSIs, Computer Operations, Network/Telecom Personnel, Strategic Support, MBI Director, and all MBI agents including agents from agencies other than OPD.

9. OPD SED MASTER – This group shall include the Captain and Lieutenant of DED.

10. OPD SED – This group shall include all personnel assigned to DED, DED Task Force Agents, the Chief of Police, all Deputy Chiefs, the Staff Inspections Unit, the MBI lieutenant, and both MBI sergeants.

11. OPD EXPLORERS – This shall include all active explorers. The explorer advisor or the Criminal Investigations Division (CID) Commander as seen fit may modify this group.

12. OPD IA RESTRICTED DUTY FOR NWCPO – This group shall include any officer relieved of duty and working at the Northwest Community Police Office (NWCPO).

13. OPD IA RESTRICTED DUTY FOR SECPO – This group shall include any officer relieved of duty and working at the Southeast Community Police Office (SECPO).

14. OPD IA RESTRICTED DUTY – This group will be assigned on a case-to-case basis as determined by Internal Affairs. This group shall include all persons relieved of duty or on alternative duty. The Internal Affairs Section Manager will hold five keys marked "IA." Note: It is the responsibility of the IA Section Manager to forward a copy of the key log to the Support Services Manager on a monthly basis.

15. OPD INTELLIGENCE – This group shall include all personnel assigned to the Intelligence Unit including any TDY position, the Chief of Police, the Deputy Chief of Investigative Services, and the officer on loan to the FBI.

16. OPD INTERNAL AFFAIRS – This group shall include all personnel assigned to Internal Affairs even if on a TDY assignment, the Chief of Police, all Deputy Chiefs, the Staff Inspections Unit, and the Division Commander of Professional Standards.

17. OPD INTERNS – This group shall include all interns regardless of the area of assignment. The Support Services Manager may change the intern access on a case-by-case basis.

18. OPD LEGAL ADVISOR INTERNS – This group shall include any intern assigned to the Legal Advisor's office.

19. OPD MASTER – This group shall include the Chief of Police, all Deputy Chiefs, and the Inspections Unit per the current issue of P&P 2106, Staff Inspections Unit.

20. OPD MBI DIRECTOR – This group shall only include the MBI Director.

21. OPD MOTOROLA – This group shall include any Motorola representative.

22. OPD NETWORK AND TELECOM – This group shall include all Network and Telecommunications personnel assigned by City Hall's Network Support Manager.

23. OPD ORANGE COUNTY PUBLIC SAFETY – This group shall include all Orange County Public Safety personnel who work on the radio tower.

24. OPD OTHER MBI (NON-OPD) – This group shall include all other MBI agency agents other than OPD personnel.

25. OPD PROPERTY & EVIDENCE MAIN VAULT – This group shall include employees who work directly with the Property & Evidence main vault.

26. OPD PROPERTY & EVIDENCE VAULTS – This group shall include only employees who work directly with evidence.

27. OPD PROPERTY & EVIDENCE – This group shall include all assigned Property & Evidence personnel

28. OPD RETIREES – This group shall include all OPD retirees granted access to OPH by the Chief of Police.

29. OPD SECPO MAINTENANCE – This group shall include any maintenance card with access only into the Southeast Community Police Office.

30. OPD STRATEGIC SUPPORT – This group shall include both TM Strategic Support persons from City Hall on loan to OPD, City Hall's Deputy Chief Information Officer, and the City's Information Security Administrator.

31. OPD SUPPORT AND CHAPLAINS – This group shall include Chaplains, recruits (non-sworn), administrative support staff, and Legal Advisor's office.

32. OPD SWORN – This group shall include all sworn and reserve officers.

33. OPD TECHNOLOGY MANAGEMENT CSSAs – This group shall include both City Hall CSSAs and their backup on loan to OPD from City Hall per the Computer Operations Manager at City Hall.

34. OPD VENDOR – This group shall include any vendor with an assigned access card.

35. OPD VOLUNTEERS – This group shall include all active volunteers. The Support Services Manager, with the approval of the Community Relations Division Commander, may change this access on a case-by-case basis.

36. ORLANDO OPERATIONS CENTER (OOC COMMUNICATIONS CENTER) – This group shall include all OPD and OFD personnel assigned to the Communications Center.

7. SUPPORT SERVICES MANAGER

7.1 RESPONSIBILITY

The Support Services Manager will be in charge of the card reader access system. The Support Services Manager will work closely with the City's Information Security Administrator. It shall be the responsibility of the Support Services Manager to maintain the card reader access system with any repairs to the system, battery backup or new installs. Additionally, it is the requesting Division Commander or Manager's responsibility to ensure that the proper foundation is in place for any new installations including backup batteries for all buildings without a generator. It is the responsibility of each Division Commander over a community police office without a generator to plan for the budget of the 48-hour backup batteries.

7.2 SYSTEM CHANGES AND UPGRADES

The Support Services Manager will go through Facilities Management on all installs requiring the use of the network system or any additions made to the system. The designated purchasing agent, along with the Technology Management Systems and Facilities Management, will oversee the ongoing annual contract for the electronic system's maintenance.

8. SITE ADMINISTRATOR

The only designated site administrator will be at OPH, located in the ID Unit. The site administrator/designee will be able to create new badges for new employees and handle an access card modification per the request of the sworn or civilian Division Commander (i.e., transfer per Section 4.2.)

9. SEPARATION

Any person who has an access card issued to them must return it upon separation from the Orlando Police Department, or any unit associated with OPD (e.g., MBI). The following groups must return their access card to their supervisor. The supervisor must then return the card to the ID unit within 24 hours from time of separation as well as notify the Support Services Manager.

1. Academy Recruits (non-sworn)
2. Chaplains
3. Citizen Observer Program
4. Citizen Police Academy Alumni
5. Crimeline
6. Explorers
7. Interns (regardless of assigned unit)
8. MBI Agents (other than OPD employees)
9. Reserves
10. Retirees
11. Volunteers
12. Traffic Control Specialist

If an access card is not returned within 24 hours of a separation, the Support Services Manager must be notified via email immediately so further action can be taken.

ATTACHMENT A

ORLANDO POLICE DEPARTMENT
VENDOR TEMPORARY ACCESS CARD ISSUE LOG

NAME (PLEASE PRINT)	DEPARTMENT	ACCESS CARD #	VEN #	ISSUE DATE	RETURN DATE	EMPLOYEE INITIALS	Property Clerk EMP. # of ISSUING PARTY	Property Clerk EMP. # of RECEIVING PARTY

ATTACHMENT B

OPD DAILY TEMPORARY VISITOR PASS LOG

DATE_____

PASS #	TRAINING RED / VENDOR GREEN / LAW ENFORCEMENT BLUE / GENERAL VISITOR YELLOW	NAME (PLEASE PRINT)	TIME	OPD EMPLOYEE/ESCORT AND FLOOR #	ID (IF NO ID, USE NONE)	PASS RET. ✔

EMPLOYEE ONLY TO PRINT VISITOR'S NAME
USE A NEW PAGE EACH DAY. FILE DAILY PAGES IN FILE FOLDER.
FORWARD ALL PAGES TO THE SUPPORT SERVICES MANAGER AT THE END OF EACH QUARTER